

TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
THEODORE MAYA (SBN 223242)
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW*
b.barnow@barnowlaw.com
ERICH P. SCHORK*
e.schork@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312.621.2000

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

* *pro hac vice* to be submitted

*Attorneys for Plaintiffs and the Proposed
Classes*

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

RICKY COCHRAN and ALAIN BERREBI,
individually and on behalf of all others similarly
situated,

Plaintiffs,

v.

THE KROGER CO. and ACCELLION, INC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Ricky Cochran and Alain Berrebi (“Plaintiffs”), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Accellion, Inc. (“Accellion”) and The Kroger Co. (“Kroger”) (together, “Defendants”).

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals (“Class Members”) who had their sensitive personal information—including but not limited to names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers (SSN), bank account and routing information, information used to process health insurance claims, and prescription information¹ (collectively, “Personal Information”)—disclosed to unauthorized third parties during a data breach compromising Accellion’s legacy File Transfer Appliance software (the “Data Breach”).

2. Accellion made headlines in late 2020/early 2021 (and continues to receive a raft of negative publicity) following its December 23, 2020 disclosure to numerous clients that criminals breached Accellion’s client-submitted data via a vulnerability in its represented “secure” file transfer application.²

3. Accellion is a software company that provides third-party file transfer services to clients. Accellion makes and sells a file transfer service product called the File Transfer Appliance (“FTA”). Accellion’s FTA is a 20-year-old, obsolete, “legacy product” that was “nearing end-of-life”³ at the time of the Data Breach, thus leaving it vulnerable to compromise and security incidents.

4. During the Data Breach, unauthorized persons gained access to Accellion’s clients’ files by exploiting a vulnerability in Accellion’s FTA platform.

5. On February 19, 2021, Kroger publicly confirmed that the Personal Information of Kroger pharmacy customers, along with “certain associates’ HR data . . . and certain money services records,” was compromised in the well-publicized Data Breach of its file transfer software vendor, Accellion.

¹ Rich Barak, *NEW: Kroger data breach investigation continues*, ATLANTA. NEWS. NOW. (Feb. 21, 2021), <https://www.ajc.com/news/breaking-kroger-advises-customers-of-data-breach-affecting-pharmacy/R44FKCSVLNDTJHA53ON36HO2CA/> (last visited Mar. 11, 2021).

² Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger*, GIZMODO (Feb. 11, 2021, 8:47 P.M.), <https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357> (last visited Mar. 11, 2021).

³ ACCELION, *Accellion Responds to Recent FTA Security Incident* (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/> (last visited Mar. 11, 2021).

6. In a press release, Kroger identified that, inter alia, customers of Kroger Health and Money Services were impacted.⁴ Little information is available about the disclosure of Kroger employee and money service customer records, but reports indicate more specifically that pharmacy customers of The Little Clinic, Kroger Pharmacies, and Kroger's family of pharmacies operated by Ralphs Grocery Company and Fred Meyer Stores Inc. are all potentially impacted by the Data Breach. Other affiliated pharmacies possibly impacted by the Data Breach include Jay C Food Stores, Dillon Companies, LLC, Baker's, City Market, Gerbes, King Soopers, Quality Food Centers, Roundy's Supermarkets, Inc., Copps Food Center Pharmacy, Mariano's Metro Market, Pick 'n Save, Harris Teeter, LLC, Smith's Food and Drug, Fry's Food Stores, Healthy Options, Inc., Postal Prescription Services, and Kroger Specialty Pharmacy.⁵

7. On January 23, 2021, Accellion informed Kroger that Kroger's files and information were impacted by the Data Breach. Specifically, Accellion notified Kroger that an unauthorized person gained access to certain Kroger files by exploiting a vulnerability in Accellion's FTA platform.

8. At the time of the Data Breach, Kroger, along with reportedly thousands of others, was a client of Accellion. Accellion's services to Kroger, and the other customers, included the use of Accellion's outdated and vulnerable FTA platform for large file transfers. The Personal Information of Kroger's pharmacy customers, employees, and money service customers, among others, was accessed by and disclosed to criminals without authorization because who were able to exploit vulnerabilities in Accellion's FTA product.

9. Defendants were well aware of the data security shortcomings in Accellion's FTA product. Nevertheless, Defendants continued to use FTA, putting Kroger's customers and employees at risk of being impacted by a breach.

⁴ The Kroger Co., *Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers*, CISION PR NEWSWIRE (Feb. 19, 2021, 4:05 P.M.), <https://www.prnewswire.com/news-releases/accellion-security-incident-impacts-kroger-family-of-companies-associates-and-limited-number-of-customers-301231891.html> (last visited Mar. 9, 2021).

⁵ Chris Mayhew, *Kroger advises customers of a data breach affecting pharmacy and Little Clinic*, CINCINNATI.COM | THE ENQUIRER (Feb. 19, 2021, 8:34 P.M.), <https://www.cincinnati.com/story/news/2021/02/19/kroger-warns-customers-medical-prescriptions-data-breach/4514664001/> (last visited Mar. 11, 2021).

10. Defendants' failures to ensure that the file transfer services and products used by Kroger were adequately secure fell far short of their obligations and Plaintiffs' and Class Members' reasonable expectations for data privacy, jeopardized the security of Plaintiffs' and Class Members' Personal Information, and put Plaintiffs and Class Members at serious risk of fraud and identity theft.

11. As a result of Defendants' conduct and the resulting Data Breach, Plaintiffs and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

12. Plaintiff Ricky Cochran is a citizen of the state of Georgia and resides in Covington, Georgia. Believing Kroger would implement and maintain reasonable security and practices to protect his Personal Information, Mr. Cochran routinely provided his Personal Information to a Kroger pharmacy location on Salem Road in Covington, Georgia, in connection with having prescriptions filled. On or about February 19, 2021, Kroger sent Plaintiff Cochran, and Plaintiff Cochran received, a letter confirming that his personal information was impacted by the Data Breach. In the letter, Kroger identified that the nature of the information involved includes "names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers, information to process insurance claims, prescription information such as prescription number, prescribing doctor, medication names and dates, medical history, as well as certain clinical services"

13. Plaintiff Alain Berrebi is a citizen of the state of California and resides in Los Angeles, California. Believing Kroger would implement and maintain reasonable security and practices to protect his Personal Information, Mr. Berrebi routinely provided his Personal Information to a Ralphs pharmacy location on West 9th Street in downtown Los Angeles, California, in connection with having prescriptions filled. On or about March 11, 2021, Kroger sent Plaintiff Berrebi, and Plaintiff Berrebi received, a letter confirming that his personal information was impacted by the Data Breach. In the letter, Kroger identified that the nature of the information involved includes "names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers, information to process insurance

claims, prescription information such as prescription number, prescribing doctor, medication names and dates, medical history, as well as certain clinical services”

14. Defendant Accellion Inc. is a Delaware corporation with corporate headquarters located at 1804 Embarcadero Road, Suite 200, Palo Alto, California 94303.

15. Defendant The Kroger Co. is an Ohio corporation with its corporate headquarters located at 1014 Vine Street, Cincinnati, Ohio 45202.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars (\$5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendants.

17. The Court has personal jurisdiction over Defendants because Accellion has a principal office in California, Defendants conduct significant business in California, and Defendants otherwise have sufficient minimum contacts with and intentionally avail themselves of the markets in California.

18. Venue properly lies in this judicial district because, *inter alia*, Accellion has a principal place of business in this district; Defendants transact substantial business, have agents, and are otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiffs’ claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Accellion and its Unsecure File Transfer Platform, FTA

19. Accellion is a Palo Alto-based software company that makes, markets, and sells file transfer platforms and services.

20. Accellion touts its products and services as “prevent[ing] data breaches”⁶ and as being secure. On its website, Accellion states:

⁶ ACCELLION, *About Accellion*, <https://www.accellion.com/company/> (last visited Mar. 9, 2021).

1 The Accellion enterprise content firewall *prevents data breaches and compliance violations*
 2 *from third party cyber risk. CIOs and CISOs rely on the Accellion platform for complete*
 3 *visibility, security and control over . . . sensitive content* across email, file sharing, mobile,
 4 enterprise apps, web portals, SFTP, and automated inter-business workflows.⁷

5 21. Accellion also touts its commitment to data privacy, claiming that “[d]ata privacy is a
 6 fundamental aspect of the business of Accellion”⁸

7 22. Accellion markets its products and services as capable of safely transferring sensitive
 8 Personal Information through file sharing, claiming that “[w]hen employees click the Accellion button,
 9 they know it’s the *safe, secure* way to share sensitive information. . . .”⁹

10 23. Despite these assurances and claims, Accellion failed to offer safe and secure file transfer
 11 products and services and failed to adequately protect Plaintiffs’ and Class Members’ Personal
 12 Information entrusted to it by Accellion’s clients, including Kroger.

13 24. Accellion’s FTA product, which Kroger and certain of its other clients used, was not
 14 secure and, by Accellion’s own acknowledgment, outdated.

15 25. The FTA—or File Transfer Appliance—is Accellion’s twenty-year-old “legacy” file
 16 transfer software, which purportedly is designed and sold for large file transfers.¹⁰

17 26. Accellion’s FTA is an obsolete “legacy product” that was “nearing end-of-life,”¹¹ thus
 18 leaving it vulnerable to compromise and security incidents. Accellion acknowledged that the FTA
 19 program is insufficient to keep file transfer processes secure “in today’s breach-filled, over-regulated
 20

21 ⁷ *Id.* (emphasis added).

22 ⁸ ACCELLION, *Accellion Privacy Policy*, <https://www.accellion.com/privacy-policy/> (last visited Mar.
 23 11, 2021).

24 ⁹ ACCELLION, *About Accellion*, <https://www.accellion.com/company/> (last visited Mar. 11, 2021)
 25 (emphasis added).

26 ¹⁰ ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021),
<https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/>
 27 (last visited Mar. 11, 2021).

28 ¹¹ ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1,
 2021), [https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-](https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/)
[security-incident/](https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/) (last visited Mar. 11, 2021).

world” where “you need even broad protection and control.”¹² On the page dedicated to Accellion FTA, Accellion’s website states: “End-of-Life Announced for FTA. No Renewals After April 30, 2021.”¹³

27. Key people within Accellion have acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion’s Chief Marketing Officer Joel York confirmed that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: “It just wasn’t designed for these types of threats”¹⁴

28. Accellion’s Chief Information Security Officer Frank Balonis stated: “Future exploits of [FTA] . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible.”¹⁵

29. Despite knowing that FTA left Accellion’s customers (like Kroger) and third parties interacting and transacting with its customers (like Plaintiffs and Class Members) exposed to security threats, Accellion continued to offer and Kroger continued to utilize the FTA file transfer product at the time of the Data Breach.

C. The Data Breach

30. On December 23, 2020, the inevitable happened: Accellion confirmed to numerous clients that it experienced a massive security breach whereby criminals were able to gain access to sensitive client data via a vulnerability in its FTA platform.¹⁶

¹² ACCELLION, *Accellion FTA*, <https://www.accellion.com/products/fta/> (last visited Mar. 11, 2021).

¹³ *Id.*

¹⁴ Jim Brunner & Paul Roberts, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington State Auditor*, SEATTLE TIMES (Feb. 3, 2021, 4:57 P.M.), <https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/> (last visited Mar. 9, 2021).

¹⁵ ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/> (last visited Mar. 11, 2021).

¹⁶ Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger*, GIZMODO (Feb. 11, 2021, 8:47 P.M.), <https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357> (last visited Mar. 11, 2021).

31. According to reports, the criminals exploited as many as four vulnerabilities in Accellion's FTA to steal sensitive data files associated with up to 300 of Accellion's clients, including corporations, law firms, banks, universities, and other entities.

32. With respect to how Accellion's FTA was compromised, one report indicates:

The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.¹⁷

33. The criminals, reportedly associated with the well-known Clop ransomware gang, the FIN11 threat group, and potentially other threat actors, launched the attacks in mid-December 2020. The attacks continued from at least mid-December 2020 and into January 2021, as these actors continued to exploit vulnerabilities in the FTA platform. Following the attacks, the criminals resorted to extortion, threatening Accellion's clients, e.g., by email, with making the stolen information publicly available unless ransoms were paid.¹⁸ In at least a few instances, the criminals carried these threats and published private and confidential information online. *See id.*

34. An example of a message sent by the criminals to a client of Accellion that was victimized during the breach is below¹⁹:

¹⁷ Jai Vljayan, DARKReading, *Accellion Data Breach Resulted in Extortion Attempts Against Multiple Victims* (Feb. 22, 2021, 4:50 P.M.), <https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226> (last visited Mar. 11, 2021).

¹⁸ Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang*, BLEEPINGCOMPUTER (Feb. 22, 2021, 9:06 A.M.), <https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/> (last visited Mar. 11, 2021).

¹⁹ *Id.*

Hello!

Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address [http://\[redacted\].onion/](http://[redacted].onion/) - use TOR browser or [http://\[redacted\].onion.dog/](http://[redacted].onion.dog/) - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

35. Accellion has remained in the headlines through early 2021 (and continues to receive a raft of negative publicity) following its mid-December 2020 disclosure of the massive Data Breach. The list of groups and clients who used Accellion's unsecure FTA product and were impacted by the Data Breach continues to increase.

36. The list, to date, reportedly includes:

- Allens
- American Bureau of Shipping ("ABS")
- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Jones Day
- The Kroger Co.
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys

- The Reserve Bank of New Zealand
- Singtel
- Southern Illinois University School of Medicine
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- The University of Colorado

C. Kroger Announces It Was Impacted by the Accellion Data Breach

37. Touting itself as “one of the world’s largest retailers,” Kroger operates approximately 2,750 grocery retail stores under a variety of Banner names, including Ralphs. Kroger also operates 2,256 pharmacies located in these stores.

38. On February 19, 2021, Kroger publicly confirmed that the Personal Information of Kroger pharmacy customers, along with “certain associates’ HR data . . . and certain money services records,” was compromised in the Data Breach. Kroger specifically identified that customers of Kroger Health and Money Services were impacted.²⁰

39. On its website, Kroger provides the following, in pertinent part²¹:

Information About the Accellion Incident

Kroger has confirmed that it was impacted by the data security incident affecting Accellion, Inc. Accellion’s services were used by Kroger, as well as many other companies, for third-party secure file transfers. Accellion notified Kroger that an unauthorized person gained access to certain Kroger files by exploiting a vulnerability in Accellion’s file transfer service.

Here are the facts as we understand them: The incident was isolated to Accellion’s services and did not affect Kroger’s IT systems or any grocery store systems or data. No

²⁰ The Kroger Co., *Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers*, CISON PR NEWSWIRE (Feb. 19, 2021, 4:05 P.M.) <https://www.prnewswire.com/news-releases/accellion-security-incident-impacts-kroger-family-of-companies-associates-and-limited-number-of-customers-301231891.html> (last visited Mar. 11, 2021).

²¹ KROGER, *Accellion Incident*, <https://www.kroger.com/i/accellion-incident> (last visited Mar. 11, 2021).

credit or debit card (including digital wallet) information or customer account passwords were affected by this incident. After being informed of the incident's effect on January 23, 2021, Kroger discontinued the use of Accellion's services, reported the incident to federal law enforcement, and initiated its own forensic investigation to review the potential scope and impact of the incident.

* * *

What information may have been involved?

At this time, based on the information provided by Accellion and our own investigation, Kroger believes the categories of affected data may include certain associates' HR data, certain pharmacy records, and certain money services records.

40. While little information is currently available about the disclosure of Kroger's employee and money service customer records, reports indicate that the breach was extensive insofar as its impact on Kroger's pharmacy customers, including customers of The Little Clinic, Kroger Pharmacies, and Kroger's family of pharmacies operated by Ralphs Grocery Company and Fred Meyer Stores Inc., all of which are potentially impacted by the Data Breach. Other affiliated pharmacies possibly impacted by the Data Breach include Jay C Food Stores, Dillon Companies, LLC, Baker's, City Market, Gerbes, King Soopers, Quality Food Centers, Roundy's Supermarkets, Inc., Copps Food Center Pharmacy, Mariano's Metro Market, Pick N Save, Harris Teeter, LLC, Smith's Food and Drug, Fry's Food Stores, Healthy Options, Inc., Postal Prescription Services, and Kroger Specialty Pharmacy.²²

41. Kroger's submissions to California's Attorney General indicate that the following information of pharmacy customers was compromised in the Data Breach: "certain names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers, information to process insurance claims, prescription information such as prescription number, prescribing doctor, medication names and dates, medical history, as well as certain clinical services, such as whether [the customer] ordered an influenza test."²³

²² Chris Mayhew, *Kroger advises customers of a data breach affecting pharmacy and Little Clinic*, CINCINATI.COM | THE ENQUIRER (Feb. 19, 2021, 5:38 P.M.), <https://www.cincinnati.com/story/news/2021/02/19/kroger-warns-customers-medical-prescriptions-data-breach/4514664001/> (last visited Mar. 11, 2021).

²³ California Attorney General, *Notices of Data Breach* at 7 (Feb. 19, 2021), <https://oag.ca.gov/system/files/All%20Notices.pdf> (last visited Mar. 11, 2021).

42. According to Kroger, on January 23, 2021, Accellion notified Kroger that an unauthorized person(s) gained access to Kroger's files containing Plaintiffs' and Class Members' Personal Information by exploiting a vulnerability in Accellion's FTA.

43. The incident reportedly did not affect Kroger's IT systems and is isolated to Accellion's services. Kroger claims that it has discontinued the use of Accellion's services, reported the incident to federal law enforcement, and initiated its own forensic investigation to review the potential scope and impact of the incident.²⁴

44. Kroger's public statement also states that it is working to notify and will offer free credit monitoring to potentially impacted customers.²⁵

D. Impact of the Data Breach

45. The actual extent and scope of the impact of the Data Breach on Kroger's pharmacy and money service customers remains uncertain.

46. Kroger has confirmed that it has stopped using Accellion's services, but unfortunately for Plaintiffs and Class Members, the damage is already done.

47. Kroger has known that the FTA software is unsecured and should no longer be used in connection with data transfers. Indeed, "[m]ultiple cybersecurity experts . . . highlight that Accellion FTA is a 20-year-old application designed to allow an enterprise to securely transfer large files but it is nearing the end of life," and that "Accellion asked its customers late last year to switch over to a new product it offers called kiteworks."²⁶ On information and belief, Kroger failed to make the switch to kiteworks and knowingly continued to use FTA, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

²⁴The Kroger Co., *Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers*, CISION PR NEWswire (Feb. 19, 2021, 4:05 P.M.), <https://www.prnewswire.com/news-releases/accellion-security-incident-impacts-kroger-family-of-companies-associates-and-limited-number-of-customers-301231891.html> (last visited Mar. 11, 2021).

²⁵ *Id.*

²⁶ Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021, 6:17 A.M.), <https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/> (last visited Mar. 15, 2021).

48. The harm caused to Plaintiffs and Class Members by the Data Breach is already apparent. As identified herein, criminal hacker groups already are threatening Accellion's clients with demands for ransom payments to prevent sensitive Personal Information from being disseminated publicly.

49. Even if companies, like Kroger, that were impacted by the Accellion Data Breach pay these ransoms, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive Personal Information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

50. The Data Breach was particularly damaging given the nature of Accellion's FTA. In the words of one industry expert: "[The] vulnerabilities [in Accellion's FTA] are particularly damaging, because in a normal case an attacker has to hunt to find your sensitive files, and it's a bit of a guessing game, but in this case the work is already done . . . By definition everything sent through Accellion was pre-identified as sensitive by a user."²⁷

51. The Data Breach creates a heightened security concern for Plaintiffs and Class Members because SSNs and sensitive health and prescription information was included. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

52. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."²⁸

53. Defendants had a duty to keep Plaintiffs' and Class members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their

²⁷ Lily Hay Newman, *The Accellion Breach Keeps Getting Worse—and More Expensive*, WIRED.COM (Mar. 8, 2021, 7:00 A.M.), <https://www.wired.com/story/accellion-breach-victims-extortion/> (quoting Jake Williams, founder of the security firm Rendition Infosec) (last visited Mar. 10, 2021).

²⁸ *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html (last visited Mar. 11, 2021).

1 Personal Information to Kroger with the understanding that Kroger and any business partners to whom
 2 Kroger disclosed the Personal Information (i.e., Accellion) would comply with their obligations to keep
 3 such information confidential and secure from unauthorized disclosures.

4 54. Defendants' data security obligations were particularly important given the substantial
 5 increase in data breaches—particularly those involving health information—in recent years, which are
 6 widely known to the public and to anyone in Accellion's industry of data collection and transfer.

7 55. Data breaches are by no means new and they should not be unexpected. These types of
 8 attacks should be anticipated by companies that store sensitive and personally identifying information,
 9 and these companies must ensure that data privacy and security is adequate to protect against and prevent
 10 known attacks.

11 56. It is well known amongst companies that store sensitive personally identifying
 12 information that sensitive information—like the SSNs and prescription and other health information
 13 stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business*
 14 *Insider* noted that “[d]ata breaches are on the rise for all kinds of businesses, including retailers
 15 Many of them were caused by flaws in . . . systems either online or in stores.”²⁹

16 57. Identity theft victims are frequently required to spend many hours and large amounts of
 17 money repairing the impact to their credit. Identity thieves use stolen personal information for a variety
 18 of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

19 58. There may be a time lag between when sensitive personal information is stolen and when
 20 it is used. According to the GAO Report:

21 [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to*
 22 *a year or more before being used to commit identity theft.* Further, once stolen data have
 23 been sold or posted on the Web, *fraudulent use of that information may continue for*
 24 *years.* As a result, studies that attempt to measure the harm resulting from data breaches
 cannot necessarily rule out all future harm.³⁰

25 _____
 26 ²⁹ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies*
 27 *recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.),
<https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1> (last visited
 Mar. 11, 2021).

28 ³⁰ *Id.* at 29 (emphasis added).

59. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.³¹

60. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the “cyber black-market” for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other Personal Information directly on various illegal websites making the information publicly available, often for a price.

61. A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.³² Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

62. Medical information is especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, “[a] stolen medical identity has a \$50 street value – whereas a stolen social security number, on the other hand, only sells for \$1.”³³ In fact, the medical industry has experienced disproportionately higher instances of computer theft than any other industry.

³¹ See FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited Mar. 11, 2021)

³² See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims> (last visited Mar. 11, 2021).

³³ Study: Few Aware of Medical Identity Theft Risk, CLAIMS JOURNAL (June 14, 2012), <http://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited Mar. 11, 2021).

63. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect Accellion's FTA from being breached and to properly phase out the unsecure FTA platform, leaving Accellion's clients and its clients' customers and employees exposed to risk of fraud and identity theft.

64. Accellion is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing its file transfer services is highly sensitive. As a company that provides file transfer services involving highly sensitive and identifying information, Accellion is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

65. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with failing to ensure that Accellion's FTA was adequately secured, or phasing out the platform altogether.

66. Despite the well-known risks of hackers and cybersecurity intrusions, Defendants failed to employ adequate data security measures in connection with Kroger's use of Accellion's FTA platform in a meaningful way in order to prevent breaches, including the Data Breach.

67. The security flaws inherent to Accellion's FTA file transfer platform—and continuing to market and sell a platform with known, unpatched security issues—run afoul of industry best practices and standards. Had Accellion adequately protected and secured FTA, or stopped supporting the product when it learned years ago about its vulnerabilities, it could have prevented the Data Breach.

68. Despite the fact that Accellion was on notice of the very real possibility of data theft associated with the FTA platform, it still failed to make necessary changes to the product or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the FTA platform's disclosure of Plaintiffs' and Class members' Personal Information to criminals.

69. Defendants permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

70. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen

through a data breach that means you were somewhere out of compliance” with payment industry data security standards.³⁴

71. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

72. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach.

73. As a result of Accellion’s failure to ensure that its FTA product was protected and secured, or to phase out the platform upon learning of FTA’s vulnerabilities, the Data Breach occurred. As a result of the Data Breach, Plaintiffs’ and Class Members’ privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

74. Plaintiffs brings this action on behalf of themselves and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

Nationwide Class

All residents of the United States whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

³⁴ Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), <http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY> (last visited Mar. 11, 2021).

California Class

All residents of California whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

California Medical Information Class

All residents of California whose Medical Information³⁵ was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

Georgia Class

All residents of Georgia whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

75. Excluded from the Classes are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

76. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appear to include many thousands of members who are geographically dispersed.

77. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

78. **Adequacy**: Plaintiffs' interests are aligned with the Classes they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their counsel intend

³⁵ "'Medical information' means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j). "'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." *Id.*

1 to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiffs and
2 undersigned counsel.

3 79. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and
4 efficiently adjudicate Plaintiffs' and other Class Member's claims. The injury suffered by each
5 individual Class Member is relatively small in comparison to the burden and expense of individual
6 prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class
7 Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could
8 afford such individual litigation, the court system could not. Individualized litigation presents a potential
9 for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to
10 all parties, and to the court system, presented by the complex legal and factual issues of the case. By
11 contrast, the class action device presents far fewer management difficulties and provides the benefits of
12 single adjudication, economy of scale, and comprehensive supervision by a single court.

13 80. **Commonality and Predominance**: The following questions common to all Class
14 Members predominate over any potential questions affecting individual Class Members:

- 15 • whether Defendants engaged in the wrongful conduct alleged herein;
- 16 • whether Defendants' data security practices and the vulnerabilities of Accellion's
- 17 FTA product resulted in the disclosure of Plaintiffs' and other Class Members'
- 18 Personal Information;
- 19 • whether Defendants violated privacy rights and invaded Plaintiffs' and Class
- 20 Members' privacy; and
- 21 • whether Plaintiffs and Class Members are entitled to damages, equitable relief, or
- 22 other relief and, if so, in what amount.

23 81. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the
24 Classes, similar or identical injuries and common law and statutory violations are involved, and common
25 questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

82. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

83. Accellion negligently sold its FTA product which it has acknowledged is vulnerable to security breaches, despite representing that the product could be used securely for large file transfers.

84. Defendants were entrusted with, stored, and otherwise had access to the Personal Information of Plaintiffs and Class Members.

85. Defendants knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiffs and Class Members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Defendants, because Accellion had previously recognized and acknowledged the data security concerns with its FTA product.

86. Defendants owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted to Defendants.

87. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security in connection Accellion's FTA product. Defendants had a duty to safeguard Plaintiffs' and Class Members' Personal Information and to ensure that its systems and products adequately protected Personal Information. Defendants breached this duty.

88. Kroger's duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that Kroger is intended to, and represents that it will, handle securely.

89. Accellion's duty of care arises from its knowledge that its customers, like Kroger, entrust to it highly sensitive Personal Information that Accellion is intended to, and represents that it will, handle securely. Only Accellion was in a position to ensure that its systems and products were sufficient to protect against breaches that exploit its FTA product and the harms that Plaintiffs and Class Members have now suffered.

90. A "special relationship" exists between Defendants, on the one hand, and Plaintiffs and Class Members, on the other hand. Defendants entered into a "special relationship" with Plaintiffs and

Class Members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiffs and Class Members.

91. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

92. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information, especially in light of the fact that for years Accellion warned of the data security concerns relating to the FTA.

93. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

94. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm.

95. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class)

96. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

97. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Kroger had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and Class Members' Personal Information.

98. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a duty to provide adequate data security practices, including in connection with its sale of its FTA platform, to safeguard Plaintiffs' and Class Members' Personal Information.

99. Pursuant to HIPAA (42 U.S.C. § 1302d et. seq.), Defendants each had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

100. Defendants breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq.*), Cal. Civ. Code § 1798.100, *et seq.*, Cal. Civ. Code § 56, *et seq.*, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA platform in order to safeguard Plaintiffs' and Class Members' Personal Information.

101. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

102. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

103. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

104. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(Against Kroger Only)
(On Behalf of Plaintiffs and the Nationwide Class)

105. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

106. Kroger, through its Ralphs branded stores and other branded stores, offered to provide pharmacy-related and medical services to Plaintiffs and Class Members in exchange for payment.

107. In connection with having their prescriptions filled and receiving medical services from Kroger, Plaintiffs and Class Members entered into implied contracts with Kroger.

108. Pursuant to these implied contracts, Plaintiffs and Class Members paid money to Kroger, whether directly or through their insurers, and provided Kroger with their Personal

1 Information. In exchange, Kroger agreed, among other things: (1) to provide pharmacy-related and
2 medical services to Plaintiffs and Class Members at its various locations; (2) to take reasonable
3 measures to protect the security and confidentiality of Plaintiffs' and Class Members' Personal
4 Information; and (3) to protect Plaintiffs' and Class Members' Personal Information in compliance
5 with federal and state laws and regulations and industry standards.

6 109. The protection of Personal Information was a material term of the implied contracts
7 between Plaintiffs and Class Members, on the one hand, and Kroger, on the other hand. Had
8 Plaintiffs and Class Members known that Kroger would not adequately protect its customers'
9 Personal Information they would not have received pharmacy-related or medical services from
10 Kroger.

11 110. Plaintiffs and Class Members performed their obligations under the implied contract
12 when they provided Kroger with their Personal Information and paid—directly or through their
13 insurers—for pharmacy-related or medical services from Kroger.

14 111. Necessarily implicit in the agreements between Plaintiffs/Class Members and Kroger was
15 Kroger's obligation to take reasonable steps to secure and safeguard Plaintiffs' and Class Members'
16 Personal Information.

17 112. Kroger breached its obligations under its implied contracts with Plaintiffs and Class
18 Members by failing to implement and maintain reasonable security measures to protect their Personal
19 Information.

20 113. Kroger's breach of its obligations of its implied contracts with Plaintiffs and Class
21 Members directly resulted in the Data Breach.

22 114. The damages sustained by Plaintiffs and Class members as described above were the
23 direct and proximate result of Kroger's material breaches of its agreements.

24 115. Plaintiffs and other Class Members were damaged by Kroger's breach of implied
25 contracts because: (i) they paid—directly or through their insurers—for data security protection
26 they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying
27 expenditures for protective and remedial services for which they are entitled to compensation; (iii) their
28 Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of

1 their Personal Information has been breached; (v) they were deprived of the value of their Personal
 2 Information, for which there is a well-established national and international market; and/or (vi) lost time
 3 and money incurred to mitigate and remediate the effects of the Data Breach, including the increased
 4 risks of identity theft they face and will continue to face.

5 **COUNT IV**
 6 **Violations of California's Consumer Privacy Act**
 7 **Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")**
 8 **(On Behalf of Plaintiff Berrebi and the California Class)**

9 116. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

10 117. The CCPA was enacted to protect consumers' Personal Information from collection and
 11 use by businesses without appropriate notice and consent.

12 118. Through the conduct complained of herein, Defendants violated the CCPA by subjecting
 13 Plaintiff Berrebi's and California Class Members' Personal Information to unauthorized access and
 14 exfiltration, theft, or disclosure as a result of Defendants' violation of their duties to implement and
 15 maintain reasonable security procedures and practices appropriate to the nature and protection of that
 16 information. Cal. Civ. Code § 1798.150(a).

17 119. In accordance with Cal. Civ. Code §1798.150(b), prior to the filing of this Complaint,
 18 Plaintiff Berrebi's counsel served Defendants with notice of these CCPA violations by certified mail,
 19 return receipt requested.

20 120. On behalf of California Class Members, Plaintiff Berrebi seeks injunctive relief in the
 21 form of an order enjoining Defendants from continuing to violate the CCPA.

22 121. If Defendants fail to agree to rectify the violations detailed above, individually and on
 23 behalf of California Class Members, Plaintiff Berrebi will seek actual, punitive, and statutory damages,
 24 restitution, and any other relief the Court deems proper as a result of Defendants' CCPA violations.

25 **COUNT V**
 26 **Violation of the California Confidentiality of Medical Information Act**
 27 **Cal. Civ. Code §§ 56, *et seq.* ("CMIA")**
 28 **(On Behalf of Plaintiff Berrebi and the California Medical Information Class)**

122. Plaintiffs reallege and incorporate paragraphs 1–115 as though fully set forth herein.

1 123. Section 56.10(a) of the California Civil Code provides that “[a] provider of health care,
2 health care service plan, or contractor shall not disclose medical information regarding a patient of the
3 provider of health care or an enrollee or subscriber of a health care service plan without first obtaining
4 an authorization[.]”

5 124. Kroger is a provider of healthcare within the meaning of Cal. Civ. Code § 56.05(d).

6 125. Accellion is a “contractor” within the meaning of Cal. Civ. Code § 56.05(d) and/or a
7 “business organized for the purpose of maintaining medical information” and/or a “business that offers
8 software or hardware to consumers . . . that is designed to maintain medical information” within the
9 meaning of Cal. Civ. Code § 56.06(a) and (b), and maintained and continues to maintain “medical
10 information,” within the meaning of Civil Code § 56.05(j), for “patients,” within the meaning of Cal.
11 Civ. Code § 56.05(k).

12 126. Plaintiff Berrebi and California Medical Information Class Members are “patients”
13 within the meaning of Cal. Civ. Code § 56.05(k) and are “endanger[ed]” within the meaning of Cal. Civ.
14 Code § 56.05(e), because Plaintiff Berrebi and California Medical Information Class Members fear that
15 disclosure of their Medical Information could subject them to harassment or abuse.

16 127. Plaintiff Berrebi and California Medical Information Class Members, as patients, had
17 their Medical Information created, maintained, preserved, and stored on Defendants’ computer networks
18 at the time of the Data Breach.

19 128. Defendants, through inadequate security, allowed an unauthorized third party to gain
20 access to Plaintiff Berrebi’s and other California Medical Information Class Members’ Medical
21 Information, without the prior written authorization of Plaintiff Berrebi’s and California Medical
22 Information Class Members, as required by Cal. Civ. Code § 56.10 of the CMIA.

23 129. Defendants violated Cal. Civil Code § 56.101 of the CMIA by failing to maintain and
24 preserve the confidentiality of Plaintiff Berrebi’s and other California Medical Information Class
25 Members’ Medical Information.

26 130. As a result of Defendants’ above-described conduct, Plaintiff Berrebi and California
27 Medical Information Class Members have suffered damages from the unauthorized disclosure and
28 release of their Medical Information.

131. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff Berrebi and California Medical Information Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Medical Information, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their Medical Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

132. Plaintiff Berrebi, individually and for each member of the California Medical Information Class, seeks nominal damages of one thousand dollars (\$1,000) for each violation under Cal. Civ. Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Cal. Civ. Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to \$3,000 per Plaintiff and California Medical Information Class Member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VI
Violations of the Georgia Fair Business Practices Act
Ga. Code §§ 10-1-390 *et seq.* ("GFBPA")
(Against Kroger Only)
(On Behalf of Plaintiff Cochran and the Georgia Class)

133. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

134. The GFBPA declares "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" to be unlawful, Ga. Code Ann. § 10-1-393(a), including but not limited to "representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have" Ga. Code Ann. § 10-1-393(b).

1 135. Defendant Kroger makes pharmacy, prescription, and other sales through its pharmacy
2 locations, holding itself out as a company that adequately provides for privacy and security of sensitive
3 Personal Information, when in reality, Kroger puts its pharmacy customers' sensitive Personal
4 Information at risk of theft as described herein.

5 136. Defendant Kroger's practices, acts, policies, and course of conduct, including its
6 omissions regarding data security and its continued use of the unsecured FTA, as described above, were
7 intended to induce, and did induce, Plaintiff Cochran and members of the Georgia Class to use and
8 continue to use Kroger's pharmacy services.

9 137. Defendant Kroger made pharmacy and other sales to Plaintiff Cochran and Georgia Class
10 members knowingly concealing that it used the unsecured FTA for file transfer, that it was not taking
11 reasonable measures to protect its pharmacy customers' Personal Information, and that Plaintiff Cochran
12 and Georgia Class Members' sensitive Personal Information was vulnerable as a result.

13 138. Defendant Kroger's conduct was deceptive and likely to mislead a reasonable
14 consumer. Defendant's aforementioned deceptive acts and practices are material, in part, because they
15 concern an essential facet of data security and privacy, which are critical considerations for consumers
16 who are deciding whether or not to do business with a pharmacy that handles and stores sensitive medical
17 and prescription information for its customers. Kroger's pharmacy sales in Georgia are consumer-
18 oriented acts and thereby fall under the Georgia's Fair Business Practices Act.

19 139. Defendant Kroger's practices, acts, policies, and course of conduct violated the Georgia's
20 Fair Business Practices Act in that:

- 21 a. At the time of making sales, Defendant Kroger knowingly misrepresented and
22 intentionally omitted and concealed material information regarding privacy and
23 data security by failing to disclose to Plaintiff Cochran and Georgia Class
24 members that it did not take adequate steps to protect their medical, prescription,
25 and other Personal Information, and failed to disclose that it continued to use
26 Accellion's FTA software, which was known to outdated;
- 27 b. Defendant Kroger engaged in materially misleading and deceptive acts by
28 continuing to make pharmacy and other related sales to the consuming public,

despite having knowledge that consumers' Personal Information was exposed and vulnerable, and that theft of that information could significantly harm consumers.

140. Defendant Kroger possessed material information about the data vulnerabilities caused by continued use of Accellion's FTA, which was known to be a "legacy" platform nearing end of life, and vulnerable to threat actors, and other information not available to Plaintiff Cochran and the Georgia Class.

141. The aforementioned conduct is and was deceptive and false and constitutes an unconscionable, unfair, and deceptive act or practice in that Defendant Kroger has, through knowing, intentional, and material omissions, concealed that its data privacy and security was inadequate and that it knowingly used unsecured file transfer software, namely the FTA platform, which put its pharmacy customers at risk of exposure.

142. As a direct and proximate result of Defendant Kroger's violations of the above, Plaintiff Cochran and Georgia Class members suffered damages including, but not limited to: (1) overpaying for prescriptions and use of Kroger's services which did not entail adequate data security and privacy, (2) lost control over sensitive Personal Information; (3) lost time addressing the consequences of the Data Breach; and (4) actual fraud or risk of future harm as a result of the theft of Personal Information due to the breach.

143. As a direct and proximate result of Kroger's unconscionable, unfair, and deceptive acts or practices, Plaintiff Cochran and Georgia Class members have been injured as alleged herein. Plaintiff Cochran will make a demand in satisfaction of Ga. Code Ann § 10-1-399(b), and may amend this Complaint to assert claims under the Georgia FBPA once the required time has elapsed. This section is included for purposes of notice only and is not intended to assert a claim under the Georgia FBPA.

COUNT VII
Violations of Georgia's Uniform Deceptive Trade Practices Act
Ga. Code §§ 10-1-370, *et seq.* ("Georgia UDTPA")
(Against Kroger Only)
(On Behalf of Plaintiff Cochran and the Georgia Class)

144. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

1 145. Defendant Kroger, Plaintiff Cochran, and Georgia Class members are “persons” within
2 the meaning of the Georgia UDTPA, Ga. Code Ann § 10-1-371(5).

3 146. The Georgia UDTPA prohibits “deceptive trade practices,” which include the
4 “misrepresentation of standard or quality of goods or services,” and “engaging in any other conduct
5 which similarly creates a likelihood of confusion or of misunderstanding.” Ga. Code Ann § 10-1-372(a).

6 147. In the course of its business, Kroger willfully failed to disclose and actively
7 concealed that it put customers’ Personal Information at risk of exposure and exposed them to identity
8 theft and fraud, and otherwise engaged in activities with a tendency or capacity to deceive, while
9 obtaining prescription and other pharmacy sales. Defendant Kroger also engaged in unlawful trade
10 practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or
11 concealment, suppression, or omission of any material fact with intent that others rely upon such
12 concealment, suppression, or omission, in connection with making sales.

13 148. Kroger knew it was using the unsecured FTA software and putting customers’ Personal
14 Information at risk of exposure, but concealed all of that information. Kroger was aware that it valued
15 profits over data security and privacy, and concealed this information as well.

16 149. Kroger’s unfair or deceptive acts or practices were likely to and did in fact deceive
17 reasonable consumers, including Plaintiffs and the other Georgia Class members, about the true nature
18 of its pharmacy services.

19 150. Defendant Kroger intentionally and knowingly misrepresented material facts regarding
20 its data security, privacy, and pharmacy sales, with an intent to mislead Plaintiffs and the Georgia Class.

21 151. Defendant Kroger knew or should have known that its conduct violated the Georgia
22 UDTPA. Indeed, it was informed by Accellion of the legacy and unsecured nature of FTA, and was told
23 that it should switch over to a more secure platform, but failed to do so.

24 152. As alleged herein, Kroger omitted material information about data security and privacy
25 with respect to Personal Information.

26 153. Defendant Kroger owed Plaintiff Cochran a duty to disclose the truth because it:
27
28

- a. Possessed exclusive knowledge that it valued profits and cost-cutting over data security and privacy;
- b. Knew it was using the unsecured FTA platform with knowledge of its vulnerabilities, and that customers' Personal Information was being exposed; and
- c. Intentionally concealed the foregoing from Plaintiffs and the Georgia Class;

154. Because Defendant Kroger fraudulently concealed the truth from Plaintiff Cochran and Georgia Class members, Plaintiff Cochran and Georgia Class members continued shopping at Kroger's pharmacy locations, unwittingly putting their Personal Information at risk of unauthorized exposure.

155. Plaintiff Cochran and the Georgia Class suffered ascertainable loss caused by Kroger's concealment of and failure to disclose material information. Class members who made pharmacy purchases at Kroger pharmacy locations would not have agreed to make those purchases or otherwise would have acted differently but for Defendant's violations of the Georgia UDTPA.

156. Kroger had an ongoing duty to all Kroger pharmacy customers to refrain from unfair and deceptive practices under the Georgia UDTPA. Plaintiff Cochran and Georgia Class members have suffered ascertainable loss as set forth herein.

157. Defendant Kroger's violations present a continuing risk to Plaintiff Cochran as well as to the general public. Defendant Kroger's unlawful acts and practices complained of herein affect the public interest.

158. As a direct and proximate result of Defendant Kroger's violations of the Georgia UDTPA, Plaintiffs and the Georgia Class have suffered injury in fact and actual damage.

159. Plaintiffs also seeks an order enjoining Defendant Kroger's unfair, unlawful, and deceptive practices, attorneys' fees, costs, and any other just and proper relief available under the Georgia UDTPA per Ga. Code Ann. § 10-1-373.

COUNT VIII
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiffs and the Nationwide Class)

160. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

161. Plaintiffs and Class Members had a reasonable expectation of privacy in the Personal Information that Defendants disclosed without authorization.

162. By failing to keep Plaintiffs' and Class Members' Personal Information safe, knowingly utilizing the unsecure FTA platform, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

- a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and
- b. invading Plaintiffs' and Class Members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;
- c. failing to adequately secure their Personal Information from disclosure to unauthorized persons;
- d. enabling the disclosure of Plaintiffs' and Class Members' Personal Information without consent.

163. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

164. Defendants knew that Accellion's FTA platform was vulnerable to data breaches prior to the Data Breach.

165. Defendants invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

166. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

167. In failing to protect Plaintiffs' and Class Members' Personal Information, and in disclosing Plaintiffs' and Class Members' Personal Information, Defendants acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

168. Plaintiffs seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representative and undersigned counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages to the maximum extent allowable;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demands a trial by jury on all issues so triable.

Dated: March 17, 2021

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (SBN 174806)

twolfson@ahdootwolfson.com

ROBERT AHDOOT (SBN 172098)

rahdoot@ahdootwolfson.com

THEODORE MAYA (SBN 223242)

tmaya@ahdootwolfson.com

AHDOOT & WOLFSON, PC

2600 W. Olive Avenue, Suite 500

Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW*
b.barnow@barnowlaw.com
ERICH P. SCHORK*
e.schork@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60602
Telephone: 312-621-2000
Facsimile: 312-641-5504

** pro hac vice to be filed*

Attorneys for Plaintiffs and the Proposed Classes